Information and Computation **152**, 44–61 (1999)
Article ID inco.1999.2788, available online at http://www.idealibrary.com on IDEAL®

Decision Trees: Old and New Results

Rudolf Fleischer*

Max-Planck-Institut für Informatik, 66123 Saarbrücken, Germany
E-mail: rudolf@mpi-sb.mpg.de

In this paper, we prove two general lower bounds for algebraic decision trees which test membership in a set $S \subseteq \mathbb{R}^n$ which is defined by linear inequalities. Let $\text{rank}(S)$ be the maximal dimension of a linear subspace contained in the closure of S (in Euclidean topology). First we show that any decision tree for S which uses products of linear functions (we call such functions mlf-*functions*) must have depth at least $n - \text{rank}(S)$. This solves an open question raised by A. C. Yao and can be used to show that mlf-functions are not really more powerful than simple comparisons between the input variables when computing the largest k out of n elements. Yao proved this result in the special case when products of at most two linear functions are allowed. Our proof also shows that any decision tree for this problem must have exponential size. Using the same methods, we can give an alternative proof of Rabin's theorem, namely that the depth of any decision tree for S using arbitrary analytic functions is at least $n - \text{rank}(S)$.

1. INTRODUCTION

Among other algebraic complexity measures (e.g. [13, 27]), the algebraic decision tree and algebraic computation tree models have turned out to be very useful in proving lower bounds for elementary combinatorial or geometric problems like maximum finding, set equality, set disjointness, and sorting (see [2] for more examples), and less elementary problems like convex polygon inclusion [20] and motion planning [18].

The algebraic decision tree model is an abstraction of "real" algorithms, where only comparisons between input variables or functions of input variables are counted, whereas all other time-consuming operations like data-management, function evaluation, or other control structures have zero cost. For complex problems, this simplification can make the problem considerably easier; for example, the knapsack problem which is known to be NP-complete has a polynomial solution in

* The author was partially supported by the EU ESPRIT LTR Project 20244 (ALCOM-IT). He was further supported by a Habilitation Scholarship of the German Research Foundation (DFG).

0890-5401/99 $30.00

the decision tree model [14]. This shows that the power of lower bound proofs in the decision tree model is quite limited.

A *decision problem* is a disjoint partition of $\mathbb{R}^n$ into sets $S_1, ..., S_q$, i.e., $\mathbb{R}^n = S_1 \cup \cdots \cup S_q$. A *decision tree* T for a decision problem is a binary tree whose internal nodes are labeled by predicates "$f(x) \diamond 0$," where $f(\ )$ is a real-valued function on $\mathbb{R}^n$ and $\diamond \in \{>, \geqslant, <, \leqslant, =, \neq\}$. The outgoing edges of an internal node are labeled by *true* or *false*, and each leaf is labeled by one of the S_i. The computation of T on input $x \in \mathbb{R}^n$ starts at the root and then proceeds downwards by evaluating the predicates at internal nodes and taking the appropriate of the two outgoing edges. This defines the *computation path* of x. When finally a leaf with label S_x is reached, S_x is the result of the computation. T is *correct* if $x \in S_x$ for all x. The worst-case *running time* of T is the length of the longest computation path in T.

T is called an *algebraic decision tree* if all functions evaluated at internal nodes are defined by polynomials. The most restricted algebraic decision trees are *comparison trees* where only comparisons between two input variables are allowed [8, 12]. *Linear decision trees* where linear functions of the input variables can be used [3, 6, 8, 12, 22, 23] are more powerful [24]. Products of two linear functions (which we call *two-linear functions*) were used in [9, 28], and arbitrary polynomials of bounded degree in [2, 20, 26]. Finally, arbitrary analytic functions were allowed in [11, 19]. Accordingly, we speak of *two-linear*, *bounded-degree* and *analytic decision trees*, respectively. A decision tree with `mlf`-*functions* (multi-linear-factor functions, i.e., arbitrary products of linear functions) is called an `mlf`-*decision tree*. Of course, this classification of algebraic decision trees is not exhaustive (see, for example, [6, 17]).

In this paper, we only consider deterministic algebraic decision trees. Probabilistic and nondeterministic decision trees [10, 12, 15, 25] and algebraic computation trees [2, 18] have also been studied.

We assume throughout this paper that the decision problem is a *membership problem*; i.e., the problem is to decide whether an input $x \in \mathbb{R}^n$ is contained in a set $S \subseteq \mathbb{R}^n$ (we call S the *target set*), but the lower bounds mentioned below can easily be transformed into similar bounds for arbitrary decision problems.

Many lower bound techniques are known for algebraic decision trees. The logarithm of the number of connected components of S is a lower bound for the depth of any linear or bounded-degree decision tree [2, 6, 20, 26]. Or one can try to prove that there must be at least one long path in the tree [6, 19], or even that all paths must be long [28]. Another approach is to prove the existence of many disjoint subtrees [8]. Topological properties of S, like the number of k-dimensional faces of S for any k [23] or the Euler characteristic of S [3, 29] have also been used to prove lower bounds.

For analytic decision trees, Rabin proved the fundamental theorem that any decision tree for S must have depth at least k if S is defined by a set of k independent linear inequalities [19]. This result was later generalized by Jaromczyk to sets S defined by arbitrary polynomial inequalities [11], however, at the cost of posing several restrictions on the polynomials (they must be irreducible, positively and negatively dense, and sign-independent; see Jaromczyk's paper for definitions).

With a different approach, Recio and Pardo obtained a less restrictive variant of this generalization [21].

Another generalization of Rabin's theorem was given by Montaña *et al.* [16]. Their paper also discusses a problem in Rabin's original paper. Rabin proved that the width of any complete proof for S (see Section 3 for definitions) must have width at least k, if S is the intersection of k "independent" half-spaces. Then he argued that the paths in a decision tree for S define a complete proof for S, so the same lower bound holds for the depth of the tree. As shown in [16], this reduction from decision trees to complete proofs is problematic.

In this paper, we give an alternative proof of Rabin's theorem which avoids the problem mentioned in [16]. Our proof is based on a new lower bound technique which we used to solve an open question raised by Yao. In [28], Yao showed that median tests are not really more powerful than simple comparisons between the input variables when computing the largest k out of n elements. He raised the question whether this can be generalized to arbitrary `mlf`-functions (note that the median test can be written as the product of two linear functions).

We give a positive answer to this question. Our proof technique is based on a dimension argument and works only for sets S defined by linear inequalities. Let $rank(S)$ be the maximal dimension of a linear subspace contained in the closure of S. We show that, for any computation path p in the decision tree, the closure of the set of inputs x which have computation path p always contains a linear subspace of dimension $n - \text{length}(p)$. Hence $\text{length}(p) \geqslant n - \text{rank}(S)$. Our proof also shows that any decision tree for this problem must have exponential *size*. The size is a much less explored measure of the complexity of decision trees versus the depth (obviously, a lower bound on the size implies a logarithmic lower bound on the depth).

The main difference between Rabin's theorem and Yao's theorem is that Rabin's theorem establishes the existence of *at least one* expensive computation path in any `mlf`-decision tree for S, whereas Yao's theorem shows that *all* paths in a `mlf`-decision tree must be expensive. Because Yao's result is much stronger than Rabin's, it is not surprising that it holds only for a much more restricted class of functions (`mlf`-functions versus analytic functions). In Yao's application of computing the k largest of n elements, the strong theorem of Yao is needed; Rabin's theorem would not give the lower bounds in Theorem 4.12.

We mention that related results can be found in the mathematics literature in the field of *real algebraic geometry*. There the problem was studied: Given an open set $S \subseteq \mathbb{R}^n$ defined by polynomial inequalities $f_1(x) > 0, ..., f_s(x) > 0$, how many polynomials are necessary and sufficient to describe S by such a system of inequalities. It turns out that d is a lower bound for s if the dimension of S is d, and 2^d is approximately an upper bound for s [1, 4, 5].

This paper is organized as follows. In Section 2 we give some geometric definitions and lemmas. In Section 3 we define certificates and proofs, an abstraction of the decision tree model. The generalization of Yao's theorem and a proof of Rabin's theorem follow in Sections 4 and 5, respectively. And we conclude with some remarks in Section 6.

2. GEOMETRIC PRELIMINARIES

In this section we give some elementary definitions. For a set $B \subseteq \mathbb{R}^n$, we denote its interior by B^0 and its closure by $\bar{B}$.[1] We call B *truly n-dimensional* if $\overline{B^0} = B$ (for example, if $B_1 = \{(x, y) \in \mathbb{R}^2 \mid x \geqslant 0, y > 0\}$ and $B_2 = B_1 \cup \{(x, y) \in \mathbb{R}^2 \mid y = 0\}$ then B_1 is truly n-dimensional, but B_2 is not truly n-dimensional). Or in other words, B is truly n-dimensional if it is the union of an open n-dimensional set and some part of its boundary. $B_n(z, \varepsilon)$ denotes the n-dimensional ball of radius ε centered at z.

A *linear variety* (*flat*) in $\mathbb{R}^n$ is a subset $G \subseteq \mathbb{R}^n$ of the form $G = v + L$, where $L \subseteq \mathbb{R}^n$ is a linear subspace and $v \in \mathbb{R}^n$. The flat has dimension $\dim G = \dim L$.

Let $L_n = \{\lambda_0 + \sum_{i=1}^n \lambda_i x_i \mid \lambda_0, ..., \lambda_n \in \mathbb{R}\}$ be the set of linear functions in n variables $x = (x_1, ..., x_n)$. Let $L_n^{(j)} = \{l_1 \cdots l_j \mid l_i \in L_n \, \forall i\}$ be the set of `mlf`-*functions of degree* j in n variables (which is a proper subset of the set of all polynomials of degree j in n variables) and $L_n^* = L_n^\infty = \bigcup_{j=1}^\infty L_n^{(j)}$.

Each $l \in L_n$ determines an oriented hyperplane $h = \{x \in \mathbb{R}^n \mid l(x) = 0\}$ with normal vector $\mathbf{n}$. Let $\Delta = \{>, \geqslant, =, \neq\}$ be the set of all comparison operators and $\Delta_> = \{>, \geqslant\}$ (since $a < 0$ iff $-a > 0$ we do not use the comparison operators "$<$" and "$\leqslant$"). For a vector $L = (l_1, ..., l_m) \in L_n^m$ of linear functions we usually denote its vector of corresponding hyperplanes by $H = (h_1, ..., h_m)$. The union of the hyperplanes in H is the *arrangement* $\mathrm{Arr}(H)$ (see [7], for example). If $\diamondsuit = (\diamondsuit_1, ..., \diamondsuit_m)$, $\diamondsuit_i \in \Delta$, is a vector of comparison operators then we define the *set of simultaneous solutions* of L with respect to $\diamondsuit$ as $S_{L, \diamondsuit} = \{x \in \mathbb{R}^n \mid l_i(x) \diamondsuit_i 0, i = 1, ..., m\}$; if $L = \varnothing$ then $S_{L, \diamondsuit} = \mathbb{R}^n$. We omit the subscript $\diamondsuit$ whenever it is clear from the context which comparison vector $\diamondsuit$ is meant.

To measure the degree of independence of the linear functions in L we define the rank of L as $\mathrm{rank}(L) = n - \dim \mathrm{span}(\mathbf{n}_1, ..., \mathbf{n}_m)$, where $\mathbf{n}_i$ is the normal vector of the hyperplane h_i defined by l_i. The following lemma shows that no linear variety contained in $\overline{S_L}$ can have a dimension higher than $\mathrm{rank}(L)$.

LEMMA 2.1 *Let $L = (l_1, ..., l_m) \in L_n^m$ be a vector of linear functions and let $\diamondsuit \in \Delta_>^m$ be a comparison vector. Let H be the vector of hyperplanes defined by the linear functions L. If $S_L \neq \varnothing$ then*

(a) *S_L contains a linear variety of dimension* $\mathrm{rank}(L)$;

(b) *$\overline{S_L}$ does not contain a linear variety of dimension* $\mathrm{rank}(L) + 1$;

(c) $\mathrm{rank}(L) = \min\{k \mid \mathrm{Arr}(H)$ *contains a k-face*$\}$, *and there is a* $\mathrm{rank}(L)$*-face of* $\mathrm{Arr}(H)$ *contained in* $\overline{S_L}$.

Proof. Let h_i be the hyperplane corresponding to the function l_i with normal vector $\mathbf{n}_i$.

(a) Let $z \in S_L$ be arbitrary and let V be a maximal linear subspace perpendicular to all normal vectors $\mathbf{n}_i$. Then $\dim V = n - \dim \mathrm{span}(\mathbf{n}_1, ..., \mathbf{n}_m) = \mathrm{rank}(L)$. Since all h_i are parallel to V, we conclude that $z + V \subseteq S_L$.

[1] We assume Euclidian topology.

(b) If V is any linear variety contained in $\overline{S_L}$ then V must be parallel to all hyperplanes h_i, i.e., perpendicular to all normal vectors $\mathbf{n}_i$. Hence $\dim V \leqslant n - \dim \operatorname{span}(\mathbf{n}_1, ..., \mathbf{n}_m) = \operatorname{rank}(L)$.

(c) Any k-face in $\operatorname{Arr}(H)$ is a k-dimensional subset of the intersection of $n-k$ linearly independent hyperplanes of H (e.g., [7]). Since there are not more than $\operatorname{span}(\mathbf{n}_1, ..., \mathbf{n}_m)$ linearly independent hyperplanes in H, $\operatorname{Arr}(H)$ contains only k-faces for $k \geqslant n - \dim \operatorname{span}(\mathbf{n}_1, ..., \mathbf{n}_m) = \operatorname{rank}(L)$. ∎

Let $L \in L_n^m$ be a vector of linear functions and H the vector of hyperplanes defined by L. Then $\operatorname{Arr}(H)$ induces a *signature* on the points $x \in \mathbb{R}^n : \operatorname{sig}(x) = (\varepsilon_1, ..., \varepsilon_m)$, where $\varepsilon_i = -, 0, +$ iff x lies under, on, above h_i, respectively. L is *sign-independent* if all possible signatures are realized in $\operatorname{Arr}(H)$. The theorems of Rabin and Jaromczyk require that the linear functions defining the target set S are sign-independent. The following lemma gives another characterization of sign-independence in terms of $\operatorname{rank}(L)$.

LEMMA 2.2. *Let $L = (l_1, ..., l_m) \in L_n^m$ and let h_i be the hyperplane defined by l_i for $i = 1, ..., m$. Then*

$$L \text{ is sign-independent} \Leftrightarrow \dim \bigcap_{i=1}^{m} h_i = n - m \Leftrightarrow \operatorname{rank}(L) = n - m.$$

Proof. Elementary geometry; see [7], for example. ∎

The definitions given so far apply to the target set S. We further need some definitions concerning the functions which are used at internal nodes of the decision tree. Yao restricted these functions to products of two linear functions, whereas Rabin allowed arbitrary analytic functions. Below, we define a general framework of function classes which includes the models of Yao and Rabin (Theorem 2.4 below).

Let $\mathscr{F}_n$ be a set of real-valued functions in n variables. We can consider any function $f(x_1, ..., x_m)$ in $m < n$ variables to be a function in n variables by adding the zero terms $0 \cdot x_{m+1} + \cdots + 0 \cdot x_n$. We call $\mathscr{F}_n$ *valid* if it satisfies properties (F1)–(F6):

If $f, g \in \mathscr{F}_n$ and h is a hyperplane in $\mathbb{R}^n$ then

(F1) f is continuous.

(F2) $f \cdot g \in \mathscr{F}_n$, i.e., $\mathscr{F}_n$ is closed under multiplication.

(F3) $\mathscr{F}_n$ is closed under translations and rotations of the coordinate system.

(F4) If there is an open set $U \subseteq \mathbb{R}^n$ with $f|_U \equiv 0$ then $f \equiv 0$.

(F5) $f|_{(x_k = 0)} \in \mathscr{F}_n$ for $k = 1, ..., n$.

(F6) If $f|_h \equiv 0$ then there exists an $g \in \mathscr{F}_n$ such that $f = l \cdot g$, where l is the linear function defining h.

LEMMA 2.3 *Then the following properties are also satisfied for* $f \in \mathscr{F}_n$:

(F7) *If* h *is a hyperplane in* $\mathbb{R}^n$ *then* $f|_h \in \mathscr{F}_n$.

(F8) *Let* V *be a linear subspace of* $\mathbb{R}^n$ *of dimension* $k \leqslant n$. *If a relatively open set* $U \subseteq V$ *exists with* $f|_U \equiv 0$ *then* $f|_V \equiv 0$.

Proof. (F7) Follows from (F3) and (F5).

(F8) V can be defined as the intersection of $n-k$ hyperplanes: $V = \bigcap_{i=1}^{n-k} h_i$. Successive application of (F7) shows that $g = f|_V$ is in $\mathscr{F}_n$. If W is a linear subspace of dimension $n - \dim(V)$ perpendicular to V then $U + W$ is open in $\mathbb{R}^n$. Since $g(x+w) = g(x)$ for $x \in V$ and $w \in W$, $g|_{U+W} \equiv (f|_V)|_U \equiv f|_U \equiv 0$ and therefore $g \equiv 0$ by (F4). ∎

THEOREM 2.4. *The following sets of functions are valid*: L_n, L_n^*, *real polynomials in* n *variables, and analytic functions in* n *variables.*

Proof. Elementary analysis. ∎

3. CERTIFICATES AND PROOFS

In this section we recall Yao's definition of certificates [28], give a definition of complete proofs which slightly differs from Rabin's definition [19], and show how these definitions are related to decision trees. We also prove a few simple geometric lemmas.

Let $L = (l_1, ..., l_m) \in L_n^m$ be a vector of linear functions, and let $\diamondsuit_L \in \Delta_>^m$ be a vector of comparison operators for L. Then the pair $(L, \diamondsuit_L)$ defines the *target set* $S_L = S_{L, \diamondsuit_L}$. Let $\mathscr{F}_n$ be a valid set of functions. These functions may be used at the internal nodes of a decision tree.

Let $G = (g_1, ..., g_k)$ be a vector of functions with $g_i \in \mathscr{F}_n$, and let $\diamondsuit_G \in \Delta^k$ be a vector of comparison operators for G. Then $S_G = S_{G, \diamondsuit_G}$ is defined analogously to before, where all g_i had been linear functions. We call the pair $Z = (G, \diamondsuit_G)$ a *certificate* for $(L, \diamondsuit_L)$ if $S_G \subseteq S_L$. The *size* of the certificate is $|Z| = k$, i.e., the number of defining functions of G. Z is *strict* if $\diamondsuit_G = \{>\}^k$. In this case we write for short $(G, >)$ or $S_{G,>}$ instead of $(G, \{>\}^k)$ or $S_{G,\{>\}^k}$, respectively. Similarly, we call the target set *strict* if $\diamondsuit_L = \{>\}^m$, and we then also use the notation $S_{L,>}$. Analogously, we write $S_{g,=}$ for the set of zeros of a function g. Since the functions in $\mathscr{F}_n$ are continuous, if $S_{G,>}$ is not empty then it is an open set and hence truly n-dimensional.

Let $Q \in \mathscr{F}_n$, $Q \not\equiv 0$, and let $Z = \{Z_1, ..., Z_p\}$ be a set of certificates. Z is a *complete proof* for $(L, \diamondsuit_L)$ with respect to Q if

(C1) Each Z_i is a certificate for $(L, \diamondsuit_L)$, i.e., for all $x \in \mathbb{R}^n$ and $i = 1, ..., k$ we have that $x \in S_{Z_i}$ implies $x \in S_L$.

(C2) S_L is covered by $S_{Q,=}$ and the S_{Z_i}, i.e., if $x \in S_L$ and $Q(x) \neq 0$ then there is an i such that $x \in S_{Z_i}$.

The *width* $|Z|$ of Z is the maximal size of one of its certificates, i.e., $|Z| = \max_i |Z_i|$. If all Z_i are strict then Z is a *strict complete proof.*

There is a strong correspondence between certificates and complete proofs on one side and decision trees on the other side. Given a decision tree which decides membership in a set $S_{L,\diamond_L}$, the set of functions evaluated along any yes-path (a path which gives the answer "is a member") is, after some sign changes, a certificate for $(L, \diamond_L)$. And the collection of all certificates corresponding to all yes-paths is a complete proof for $(L, \diamond_L)$ with respect to any function Q. Hence, any lower bound on the width of complete proofs is also a lower bound on the depth of decision trees.

Obviously, for any certificate Z there exists a decision tree with a yes-path corresponding to Z. However, it is not straightforward to construct for a given complete proof a decision tree whose set of yes-paths corresponds to the set of certificates of the complete proof.

The next two lemmas show that it is sufficient to show lower bounds for strict complete proofs. Here we differ from Rabin who only allowed nonstrict inequalities (i.e., "$\geqslant$") in the definitions of S_G and S_L. He could then give an elegant proof for the minimal width of complete proofs for S_L; however, as discussed in [16], this does not immediately give a corresponding lower bound for the depth of decision trees.

LEMMA 3.1. *Let $Z=(G, >)$ be a strict certificate for $(L, \diamond)$, where $\diamond \in \Delta^m_>$. Then Z is also a strict certificate for $(L, >)$.*

Proof. There is nothing to show if $S_G = \varnothing$. So assume $S_G \neq \varnothing$. Assume that there exists a $z \in S_G$ with $l_i(z) = 0$. Since S_G is an open set there exists an $\varepsilon > 0$ such that $B_n(z, \varepsilon) \subseteq S_G$ and, hence, $B_n(z, \varepsilon) \subseteq S_L$, a contradiction to $l_i(z) = 0$. ∎

LEMMA 3.2. *Let Z be a complete proof for $(L, \diamond_L)$ with respect to Q. Then there exist a set of certificates Z' and a function $Q' \in \mathscr{F}_n$ with $Q' \not\equiv 0$ such that $|Z'| \leqslant |Z|$ and Z' is a strict complete proof for $(L, >)$ with respect to Q'.*

Proof. Let $Z = \{Z_1, ..., Z_p\}$ with $Z_i = (G_i, \diamond_i)$, $G_i = (g_{i1}, ..., g_{ik})$, and $\diamond_i = (\diamond_{i1}, ..., \diamond_{ik})$. We define $Q' = Q \cdot \prod_{i,j} g_{ij}$, where the product is taken over all $g_{ij} \not\equiv 0$. Since $Q \not\equiv 0$, we have $Q' \not\equiv 0$. We define Z' by

(1) replacing all predicates "$g_{ij} \neq 0$" by "$g_{ij}^2 > 0$",

(2) throwing away all Z_i with $\diamond_{ij} =$ "$=$" for some j,

(3) and finally defining all remaining $\diamond'_{ij} =$ "$>$."

Obviously, $|Z'| \leqslant |Z|$ and all certificates are strict. It remains to show that Z' is a complete proof for $(L, >)$. Step (1) is possible because of property (F2) of $\mathscr{F}_n$. So suppose w.l.o.g. that Z does not contain any "$\neq$"-comparisons.

(C1) Since $S_{Z'_i} \subseteq S_{Z_i}$ for all Z'_i remaining after step (2), the Z'_i are also certificates for $(L, \diamond_L)$ and, hence, for $(L, >)$ by Lemma 3.1.

(C2) If there is an $x \in S_{L,>}$ with $Q'(x) \neq 0$ then in particular $x \in S_L$ and $Q(x) \neq 0$. By (C2) there must be an i such that $x \in S_{Z_i}$, i.e., $g_{ij}(x) \diamond_{ij} 0$ for all j, where $\diamond_{ij} \in \{>, \geqslant, =\}$. $Q'(x) \neq 0$ implies $\diamond_{ij} \in \{>, \geqslant\}$ and $g_{ij}(x) > 0$ for all j.

Hence, Z_i was not removed in step (2) and $x \in S_{Z_i'}$; i.e., Z_i' is a strict certificate for x. ∎

We remark that in the lemma above $S_{L,>}$ might be empty, but then all certificates Z_i' in the proof would also define empty sets $S_{Z_i'}$. In Section 5 we wil prove lower bounds for strict complete proofs and then use Lemma 3.2 to extend these results to arbitrary complete proofs. We close this section with some simple geometric observations.

LEMMA 3.3 *Let $L = (l_1, ..., l_m)$ be a vector of linear functions. Let h be a hyperplane with defining function l and let x be some point on h.*

(a) *Let $C \subseteq \mathbb{R}^n$ be truly n-dimensional and let $g_1, ..., g_k \in \mathscr{F}_n$ be functions which are not vanishing identically. Then for all $y \in C$ and all $\varepsilon > 0$, there exists a z in $C^0 \cap B_n(y, \varepsilon)$ with $g_i(z) \neq 0$ for all i*; i.e., *each $y \in C$ can be slightly perturbed within C^0 to avoid the zerosets of all the g_i.*

(b) *Let $g \in \mathscr{F}_n$, $g \not\equiv 0$, with l not dividing g. Then for all $\varepsilon > 0$, there exists a z in $B_n(x, \varepsilon)$ with $l(z) \cdot g(z) > 0$.*

(c) *If an $\varepsilon > 0$ exists such that $B_n(x, \varepsilon) - h \subseteq S_{L,>}$ then $x \in S_{L,>}$.*

(d) *Let Z be a strict certificate for L. If an $\varepsilon > 0$ exists such that $h \cap B_n(x, \varepsilon) \subseteq \overline{S_Z}$ then $l_i(x) > 0$ for all $l_i \neq l$ (i.e., if some small environment of x within hyperplane h does not stick outside of S_Z then x must be a point within $S_{L,>}$, or it must lie on its boundary if h is a bounding hyperplane of $S_{L,>}$).*

Proof. (a) $C^0 \cap B_n(y, \varepsilon)$ is an open set in $\mathbb{R}^n$. Then (F4) proves the claim.

(b) (F8) and (F6) imply that there must be a $y \in h \cap B_n(x, \varepsilon/2)$ with $g(y) \neq 0$. But then $\operatorname{sgn}(g)$ is constant in $B_n(y, \gamma)$ for a $\gamma \in (0, \varepsilon/2)$. Since h divides $B_n(y, \gamma)$ into two halves with different signs of l in each half, there exists a $z \in B_n(y, \gamma) \subseteq B_n(x, \varepsilon)$ with $l(z) \cdot g(z) > 0$.

(c) Obvious.

(d) $x \in \overline{S_Z} \subseteq \overline{S_L}$ implies $l_i(x) \geqslant 0$ for all i. If $l_i(x) = 0$ and $l_i \neq l$ for an i then l_i divides the $(n-1)$-dimensional ball $h \cap B_n(x, \varepsilon)$ into two halves ($h \cap l_i$ is a $(n-2)$-dimensional hyperplane in the $(n-1)$-dimensional space h), and l_i is positive in one of the halves and negative in the other. But this contradicts $h \cap B_n(x, \varepsilon) \subseteq \overline{S_Z} \subseteq \overline{S_L}$. ∎

4. YAO'S THEOREM

In [28], Yao showed that the size of a certificate which uses only median tests is bounded from below by the number of linearly independent functions in the set L defining the target set S_L. He raised the question whether this result generalizes to certificates which use `mlf`-functions from L_n^*. In this section we show that this is the case. A partial answer to Yao's question was given by Gasarch [9] who showed that Yao's theorem still holds if products of at most two linear functions are used (i.e., functions from $L_n^{(2)}$).

THEOREM 4.1 *Let* $Z=(G, \diamondsuit_G)$, $G\in L_n^{*k}$, *and* $\diamondsuit_G\in \Delta^k$, *be a certificate for* $(L, \diamondsuit_L)$, $L\in L_n^m$. *If* $S_G\neq\emptyset$ *then* $|Z|\geqslant n-\text{rank}(L)$.

Proof. The theorem follows immediately from Lemma 2.1 and Theorem 4.3 below. ▮

COROLLARY 4.2. *Any accepting path in a decision tree for* $S_{L,\diamondsuit_L}$ *with functions from* L_n^* *must have length at least* $n-\text{rank}(L)$.

THEOREM 4.3 *Let* $G\in L_n^{*k}$ and $\diamondsuit\in\Delta^k$. *If* $S_{G,\diamondsuit}\neq\emptyset$ *then there exists a linear variety* $V\subseteq\overline{S_{G,\diamondsuit}}$ *of dimension* $n-k$.

A similar theorem for $L_n^{(2)}$ can be found in [28]. The proof of our theorem is obtained by induction on k, but due to some subtle difficulties it is much more involved than in the case of two-linear functions. The inductive step is based on the following reduction scheme.

REDUCTION 4.4 *Let* $G=(g_1, ..., g_k)\in L_n^{*k}$ and $\diamondsuit\in\Delta^k$. Let h be a hyperplane in $\mathbb{R}^n$. Then we define $G'\in L_{n-1}^{*k}$ and $\diamondsuit'\in\Delta^k$ by

$$g_i'=\begin{cases} g_i|_h & \\ \text{not existing} & \end{cases} \quad \text{iff} \quad \begin{cases} g_i|_h\not\equiv 0; \\ g_i|_h\equiv 0; \end{cases}$$

$$\diamondsuit_i'=\diamondsuit_i \quad \text{if } g_i' \text{ exists.}$$

Then obviously $|G'|\leqslant|G|$ and $g_i'(x)=g_i(x)$ for all $x\in h$. But we also need $\emptyset\neq S_{G'}\subseteq\overline{S_G}$, which is not necessarily true. In fact, this may fail for three reasons. First, if $h\cap\overline{S_G}=\emptyset$ then $S_{G'}=\emptyset$. Second, if $g_i=l^2\cdot\hat{g}_i$, where l is the defining function of h, then we discard g_i in the reduction step; but if $\diamondsuit_i=$ "$>$" then this may add points to $S_{G'}$ which are not in $\overline{S_G}$, namely all points $z\in h$ with $\hat{g}_i(z)<0$ which are not excluded by other constraints. And third, if l is a common factor of several of the g_i (which are all missing in G') then $S_{G'}$ can also be larger than $\overline{S_G}$. For example, if $Z=((x, x\cdot y, x+5), >)$ and h is the hyperplane $(x=0)$ then the reduced certificate is just $((x+5), >)$, which is true everywhere on h, whereas only the upper half of h bounds S_Z.

In the next seven lemmas we will show how to solve these problems by transforming an arbitrary certificate into a certificate of at most the same size which does not cause any of these problems. First, we will show that we can assume w.l.o.g. that certificates do not use any "$\neq$"-comparisons.

LEMMA 4.5 *Let* $G\in L_n^{*k}$ *and* $\diamondsuit\in\Delta^k$. *If* $S_{G,\diamondsuit}\neq\emptyset$ *then there exists an* $\diamondsuit'\in\Delta^k$ *such that* "$\neq$" $\notin\diamondsuit'$ *and* $\emptyset\neq S_{G,\diamondsuit'}\subseteq S_{G,\diamondsuit}$.

Proof. Let $z\in S_{G,\diamondsuit}$ be an arbitrary point. Now we define

$$\diamondsuit_i'=\begin{cases} \diamondsuit_i & \\ > & \\ < & \end{cases} \quad \text{iff} \quad \begin{cases} \diamondsuit_i\in\{>, \geqslant, =\}; \\ \diamondsuit_i=\text{ '}\neq\text{' and } g_i(z)>0; \\ \diamondsuit_i=\text{ '}\neq\text{' and } g_i(z)<0. \end{cases}$$

Then $z\in S_{G,\diamondsuit'}\subseteq S_{G,\diamondsuit}$. ▮

So we can from now on assume that $\Delta = \{>, \geqslant, =\}$. The next lemma shows that we can sometimes restrict Δ even further to $\{>\}$, i.e., we have to consider only strict certificates.

LEMMA 4.6. *Let $G \in L_n^{*k}$ and $\diamond \in \Delta^k$. If $S^0_{G,\diamond} \neq \emptyset$ then $\emptyset \neq S_{G,>} \subseteq S_{G,\diamond}$.*

Proof. $S^0_{G,\diamond} \neq \emptyset$ implies the existence of an $x \in S_{G,\diamond}$ and an $\varepsilon > 0$ such that $B_n(x, \varepsilon) \subseteq S_{G,\diamond}$. Then Lemma 3.3(a) guarantees the existence of a $z \in B_n(x, \varepsilon)$ with $g_i(z) \neq 0$ for all i. But this means $g_i(z) > 0$ for all i. Hence $z \in S_{G,>}$. ∎

The next two lemmas show how to solve the third problem for strict certificates, i.e., if the hyperplane $l(x) = 0$ is used in the reduction and l is a common factor of several of the g_i.

LEMMA 4.7. *Let $F = (l \cdot f_1, l \cdot f_2)$ and $G = (l \cdot f_1, f_1 \cdot f_2)$ with $f_1, f_2 \in \mathscr{F}_n$ and $l \in L_n$. Then $S_{F,>} = S_{G,>}$; i.e., we can replace the "bad" certificate F (with two occurrences of l) by the "good" certificate G (with only one occurrence of l), at least if l is not a factor of f_2.*

Proof.

$$\begin{aligned} x \in S_{F,>} &\Leftrightarrow l(x) \cdot f_1(x) > 0 \quad \wedge \quad l(x) \cdot f_2(x) > 0 \\ &\Leftrightarrow sgn(l(x)) = sgn(f_1(x)) = sgn(f_2(x)) \\ &\Leftrightarrow l(x) \cdot f_1(x) > 0 \quad \wedge \quad f_1(x) \cdot f_2(x) > 0 \\ &\Leftrightarrow x \in S_{G,>}. \end{aligned}$$

LEMMA 4.8. *Let $G = (g_1, ..., g_k) \in L_n^{*k}$ with $l \in L_n$ dividing g_1. Then there exists $G' = (g'_1, ..., g'_k) \in L_n^{*k}$ with $S_{G,>} = S_{G',>}$ such that l is at most a squared factor of g'_1 and does not divide any of the other g'_i, $i \geqslant 2$.*

Proof. Assume $g_i = l^{a_i} \cdot \hat{g}_i$, $a_i \in \mathbb{N}_0$ for all i. We proceed in two steps. First, we show that the multiplicities of the factor l can be made small, namely 1 or 2 for g_1, and 0 or 1 for $g_2, ..., g_k$. Then we show how to eliminate the factor l from $g_2, ..., g_k$. If there is an odd a_i we assume w.l.o.g. that a_1 is odd.

1. We define

$$g''_1 = l^{b_1} \cdot \hat{g}_1 \quad \text{with } b_1 = \begin{cases} 2 & \text{iff } \begin{cases} a_1 \text{ is even;} \\ a_1 \text{ is odd;} \end{cases} \\ 1 \end{cases}$$

and for $i = 2, ..., k$,

$$g''_1 = l^{b_1} \cdot \hat{g}_1 \quad \text{with } b_1 = \begin{cases} 0 & \text{iff } \begin{cases} a_i \text{ is even;} \\ a_i \text{ is odd;} \end{cases} \\ 1 \end{cases}$$

Then $|G| = |G''|$ and $S_{G,>} = S_{G'',>}$ which can be seen as (observe that $l^2(x) \geqslant 0$ for all $x \in \mathbb{R}^n$)

$$\begin{aligned} x \in S_{G,>} &\Leftrightarrow \forall i : g_i(x) = l^{a_i} \cdot \hat{g}_i(x) > 0 \\ &\Leftrightarrow l(x) \neq 0 \quad \wedge \quad \forall i : l^{b_i}(x) \cdot \hat{g}_i(x) > 0 \\ &\Leftrightarrow g_1''(x) > 0 \quad \wedge \quad \forall i \geqslant 2 : g_i''(x) > 0 \\ &\Leftrightarrow x \in S_{G'',>}. \end{aligned}$$

2. If $b_i = 0$ for $i \geqslant 2$ then we can choose $G' = G''$. Otherwise, $b_1 = 1$ by the assumption above. So the multiplicity of the factor l in all g_i'' is at most one. Applying Lemma 4.7 to all pairs (g_1'', g_i''), $i \geqslant 2$, where l divides g_i'' gives the desired G'. ∎

The G' constructed in the previous lemma may still have $g_1' = l^2 \cdot \hat{g}_1$ which was our second problem. The next lemma shows that we can neglect squared factors without increasing the set of solutions too much.

LEMMA 4.9. *Let $l \in L_n$ and $G = (g_1, ..., g_k) \in L_n^{*k}$ with $g_1 = l^2 \cdot \hat{g}_1$. Define G' by $g_1' = \hat{g}_1$ and $g_1' = g_i$ for $i \geqslant 2$.* Then $S_{G,>} \subseteq S_{G',>} \subseteq \overline{S_{G,>}}$.

Proof. The first inclusion is trivial. If $S_{G',>} = \emptyset$ then there is nothing to show. So let $x \in S_{G',>}$ be arbitrary. Since $S_{G',>}$ is truly n-dimensional, Lemma 3.3(a) implies the existence of a sequence $(x_i)_{i=1,2,...}$ of points $x_i \in S_{G',>}$ with $\lim_{i \to \infty} x_i = x$ and $l(x_i) \neq 0$ for all i. But this implies $x_i \in S_{G,>}$ for all i and, hence, $x \in \overline{S_{G,>}}$.

COROLLARY 4.10. *Let $G = (g_1, ..., g_k) \in L_n^{*k}$ and $l \in L_n$, dividing one of the g_i. Then a $G' \in L_n^{*k}$ exists such that $|G'| = |G|$, $S_{G,>} \subseteq S_{G',>} \subseteq \overline{S_{G,>}}$, and l is unique in G; i.e., l divides exactly one of the g_i' and l^2 does not divide any of the g_i'.*

Proof. Lemmas 4.8 and 4.9. ∎

In this case we can prove that Reduction 4.4 works properly.

LEMMA 4.11. *Let h be a hyperplane with defining function l. Let $G = (g_1, ..., g_k) \in L_n^{*k}$ such that l does not divide any of the g_i or l is unique in G. If G' is constructed by Reduction 4.4, applied to G and h, then $S_{G',>} \subseteq \overline{S_{G,>}}$.*

Proof. If l does not divide any of the g_i then $G' = G|_h$. So assume $g_1 = l \cdot \hat{g}_1$. Then g_1' does not exist. Let $x \in S_{G',>} \subseteq h$ be arbitrary. Then an $\varepsilon > 0$ exists such that $g_i(z) > 0$ for all $i \geqslant 2$ and $z \in B_n(x, \varepsilon)$. Let ε_j be a sequence of numbers with $\varepsilon \geqslant \varepsilon_j > 0$ and $\lim_{j \to \infty} \varepsilon_j = 0$. Then, by Lemma 3.3(b), there are $\hat{x}_j \in B_n(x, \varepsilon_j)$ with $g_1(\hat{x}_j) > 0$. Hence $x \in \overline{S_{G,>}}$. ∎

Proof of Theorem 4.3. Because of Lemma 4.5 we can assume that $\diamond \in \{>, \geqslant, =\}$. The proof is obtained by induction on $k = |G|$:

- $k = 1$. Let $G = \{g_1\}$. Now we have to consider two cases. Either g_1 is a product of squared factors, i.e., $g_1 = l^2 \cdot \hat{g}_1^2$ with $l \in L_n$ and $\hat{g}_1 \in L_n^*$. Then we define $V = S_{l,=}$ and have dim $V = n - 1$ and $V \subseteq \overline{S_{G,\diamond}}$.

Or g_1 has a linear factor l of odd multiplicity. Then w.l.o.g. $g_1 = l \cdot \hat{g}_1$ with $\hat{g}_1 \in L_n^*$ and l does not divide $\hat{g}_1$ (since $\operatorname{sgn}(l^3 \cdot \hat{g}_1) = \operatorname{sgn}(l \cdot \hat{g}_1)$). We define $V = S_{l,=}$. If $\diamond_1 \in \{\geqslant, =\}$ then $V \subseteq S_{G,\diamond}$. Otherwise, Lemma 3.3(b) implies that each $x \in V$ is also in $\overline{S_{G,\diamond}}$.

- $k>1$. Let $G=(g_1, ..., g_k)$, $g_i \in L_n^*$. We have to consider two cases.

  * $S^0_{G,\diamond}=\emptyset$. Let $z \in S_{G,\diamond}$ be arbitrary. Since $S^0_{G,\diamond}=\emptyset$, w.l.o.g. there exists an $l \in L_n$ such that $l(z)=0$ and $g_1 = l \cdot \hat{g}_1$. Let h be the hyperplane defined by l and let G' be constructed by Reduction 4.4, applied to G and h. Then $z \in S_{G',\diamond'}$ and $|G'|<k$. Hence, by the induction hypothesis, a linear variety $V \subseteq \overline{S_{G',\diamond'}}$ of dimension at least $(n-1)-(k-1)=n-k$ must exist.

  Hence for all $x \in V$ a sequence $(x_j)_{j=1,2,...}$ exists with $\lim_{j\to\infty} x_j = x$ and $x_j \in S_{G',\diamond'}$ for all j, i.e., $g'_i(x_j) \diamond'_i 0$ for all i, where $g'_i \in G'$ exists. All g_i which were discarded in the reduction must contain the factor l; hence, $g_i(x_j)=0$ for all these i and all j. Furthermore, $g_i(z)=0$ for all these i and, since $z \in S_{G,\diamond}$, all these $\diamond_i$ must be from $\{\geqslant, =\}$. But then $x_j \in S_{G,\diamond}$ for all j (because $g'_i = g_i|_h$ and $\diamond'_i = \diamond_i$ if it exists) and, hence, $x \in \overline{S_{G,\diamond}}$.

  * $S^0_{G,\diamond} \neq \emptyset$. Then we can assume $\diamond = \{>\}^k$ by Lemma 4.6. $S_{G,>}$ is a subset of $\mathbb{R}^n$ which is bounded by hyperplanes whose defining functions are all among the linear factors of the g_i. Let h be such a bounding hyperplane with defining function l and assume w.l.o.g. that $g_1 = l \cdot \hat{g}_1$. By Corollary 4.10, we can assume that l is unique in G.

  Let C be the $(n-1)$-face of $\overline{S_{G,>}}$ which is supported by h and let z be an arbitrary point in C^0. Then $g_1(z)=0$ and $g_i(z) \neq 0$ for all $i \geqslant 2$. Since all g_i have a constant sign in $B_n(z, \varepsilon)$ for some small $\varepsilon > 0$ (the g_i are continuous) and $z \in \overline{S_{G,>}}$, we even know that $g_i(z) > 0$ for all $i \geqslant 2$.

  Reduction 4.4, applied to G and h, gives us a G' with $g'_i(z) = g_i(z) > 0$ for all $i \geqslant 2$ (and g'_1 not existent). Hence, $z \in S_{G',>}$, i.e., $S_{G',>} \neq \emptyset$. Further, $S_{G',>} \subseteq \overline{S_{G,>}}$ by Lemma 4.11.

  Since $|G'|<k$ we have, by induction hypothesis, a linear variety $V \subseteq \overline{S_{G',>}}$ of dimension $(n-1)-(k-1)=n-k$. Therefore we know that for all $x \in V$ a sequence $(x_j)_{j=1,2,...}$ exists with $\lim_{j\to\infty} x_j = x$ and $x_j \in S_{G',>}$ for all j, i.e., $g_i(x_j) > 0$ for all $i \geqslant 2$. But then, for all j, numbers $\varepsilon_j > 0$ exist such that $g_i(z_j) > 0$ for all $z_j \in B_n(x_j, \varepsilon_j)$ and $i \geqslant 2$. We can assume w.l.o.g. that $\lim_{j\to\infty} \varepsilon_j = 0$. Since $x_j \in h$, by Lemma 3.3(b) $\hat{x}_j \in B_n(x_j, \varepsilon_j)$ exist with $g_1(\hat{x}_j) = l(\hat{x}_j) \cdot \hat{g}_1(\hat{x}_j) > 0$ and $g_i(\hat{x}_j) > 0$ for $i \geqslant 2$. Hence, $x \in \overline{S_{G,>}}$. ∎

We now apply Theorem 4.1 to the problem of finding the k largest elements, including their individual rankings, of n real numbers. Let $W_k(n)$ denote the worst-case complexity in the decision tree model when arbitrary functions from L_n^* are allowed. The following theorem generalizes Yao's theorem [28, Theorem 1] to arbitrary functions L_n^* (instead of $L_n^{(2)}$). Since Yao's proof is quite general, it can also handle our more general Theorem 4.1. For sake of completeness, we repeat a short sketch of the proof.

THEOREM 4.12. $W_k(n) \geqslant n-k+\sum_{1\leqslant i\leqslant k-1} \log(n-i+1)$ *for all* $n>k\geqslant 2$.

Proof (Sketch, see [28] for a complete proof). Let $G \in L_n^{*k}$ be a certificate for $S_L = \{x_1 - x_i \geqslant 0 \mid 2 \leqslant i \leqslant n\}$. Then $\operatorname{rank}(L)=1$ and, hence, $|G| \geqslant n-1$ by Theorem 4.1. It follows that any decision tree which finds the maximum of n numbers must have at least 2^{n-1} leaves (because each path is a certificate for maximum). Now

partition the leaves of a decision tree T which finds the k largest numbers into $\prod_{1 \leqslant i \leqslant k-1} (n-i+1)$ disjoint classes, each class containing the leaves which output $x_{i_1}, ..., x_{i_{k-1}}$ as the $k-1$ largest numbers for some fixed $i_1, ..., i_{k-1}$. Then each class induces a subtree of T which finds the maximum of $n-k$ numbers and, hence, has at least 2^{n-k} leaves. ▮

5. RABIN'S THEOREM

In [19], Rabin showed that the width of any complete proof for a sign-independent linear target set L is bounded from below by $|L|$, even if arbitrary polynomials or analytic functions are allowed in the complete proof. In this section we prove an analogous result with respect to our definition of a complete proof. We bound the width of a complete proof by $n - \text{rank}(L)$ (remember Lemma 2.2: L has rank $n-|L|$ iff it is sign-independent). Throughout this section, let $\mathcal{F}_n$ be some set of functions satisfying (F1)–(F6) (it is always possible to think of F_n as real polynomials in n variables). All certificates will use functions from F_n.

THEOREM 5.1. *Let Z be a complete proof for $(L, \diamond_L)$, $L \in L_n^m$, with respect to a function $Q \in F_n$. If $S^0_{L, \diamond_L} \neq \emptyset$ then $|Z| \geqslant n - \text{rank}(L)$.*

COROLLARY 5.2. *Any decision tree for $S_{L, \diamond_L}$ with functions from F_n must have depth at least $n - \text{rank}(L)$.*

We remark that this bound does not necessarily hold if $S^0_{L, \diamond_L} = \emptyset$. For example, $l(x) \geqslant 0$ and $-l(x) \geqslant 0$ both together are equivalent to $l(x) = 0$; hence any linear subspace V of $\mathbb{R}^n$ of dimension $k < n$ can be achieved as a target set, using a set L of $2(n-k)$ linear functions with $\text{rank}(L) = k$. But there is a trivial complete proof Z for V which consists of only one certificate, and this certificate consists of only one quadratic polynomial, i.e., $|Z| = 1$: Let $g = x_1^2 + \cdots + x_{n-k}^2$; then $S_{g, =}$ is isomorphic to $\mathbb{R}^k$.

Since $S^0_{L, \diamond_L} \neq \emptyset$, we can w.l.o.g. assume that $S_{L, >} \neq \emptyset$ and Z is a strict complete proof for $(L, >)$ by Lemma 3.2. Hence, we can also assume that all functions g_{ij} used in Z are nonzero. This makes the proofs in this section a little bit easier than in the previous section. The proof of the theorem will be obtained by induction on $|Z|$. The inductive step is based on the following reduction scheme which is an extension of Reduction 4.4.

REDUCTION 5.3. Let $Z = \{Z_1, ..., Z_p\}$ be a strict complete proof for L with respect to Q, where $Z_i = (G_i, >)$ with $G_i = (g_{i1}, ..., g_{ik}) \in \mathcal{F}_n^k$. Let h be a hyperplane. Then we define a set Z' of $(n-1)$-dimensional certificates and a new $(n-1)$-dimensional target set $S_{L'}$ by

(1) $Q' := \prod g_{ij}|_h$, where the product is taken over all g_{ij} which are not multiples of l.

(2) Z_i' is the result of Reduction 4.4 applied to Z_i and h; if $S_{Z_i'} = \emptyset$ then Z_i' is discarded.

(3) L' is the result of Reduction 4.4 applied to L and h. ▮

Then obviously $|Z'| \leqslant |Z|$. Further, $g'_{ij}(x) = g_{ij}(x)$ and $l'_i(x) = l_i(x)$ for all $x \in h$ and all i, j. If h is defined by one of the linear functions $l_i \in L$ then we even know that $|Z'| \leqslant |Z| - 1$, because each Z_i is either shortened by Reduction 4.4 or it completely vanishes (if it does not contain the factor l) as the next lemma shows.

LEMMA 5.4. *Let Z_i be a strict certificate for L and let $l \in L$ be a linear function defining a hyperplane h. If l does not divide any of the functions of Z_i then Reduction 4.4, applied to Z_i and h, yields a certificate Z'_i with $S_{Z'_i, >} = \emptyset$.*

Proof. $Z'_i = Z_i|_h$ because l does not divide any of the functions used in Z_i. Assume that an $x \in S_{Z'_i, >} \subseteq h$ exists. Then also $x \in S_{Z_i, >}$ and there exists an $\varepsilon > 0$ such that $B_n(x, \varepsilon) \subseteq S_{Z_i, >}$. But this contradicts the fact that not both sides of h can belong to S_L. ∎

It remains to show that Z' is a strict complete proof for L' with respect to Q'. Unfortunately, this is not always true as we have seen in the last section. So, once again, we need some transformations before we can prove that Reduction 5.3 works (Lemma 5.8 below). Similarly to Lemma 4.9, we first show that in a strict complete proof, squared linear factors are not important.

LEMMA 5.5. *Let $Z = \{Z_1, ..., Z_p\}$ be a strict complete proof for L with respect to Q and let $g_{ij} = l^2 \cdot \hat{g}_{ij}$ be a function used in certificate Z_i, where $l \in L_n$. We define another set of certificates Z' which only differs in Z_i by defining $g'_{ij} = \hat{g}_{ij}$. Then Z' is also a strict complete proof for L with respect to Q, and $|Z'| \leqslant |Z|$.*

Proof. $|Z'| \leqslant |Z|$ is obvious. It remains to show (C1) and (C2) for Z':

(C1) We must show that Z'_i is still a certificate for L. Obviously $S_{Z_i} \subseteq S_{Z'_i}$. Let h be the hyperplane defined by l. If $x \in h \cap S_{Z'_i}$ then there exists an $\varepsilon > 0$ such that $B_n(x, \varepsilon) \subseteq S_{Z'_i}$. But then $B_n(x, \varepsilon) - h \subseteq S_{Z_i} \subseteq S_L$ and, hence, $x \in S_L$ by Lemma 3.3(c).

(C2) $x \in S_{Z_i}$ implies $x \in S_{Z'_i}$. Therefore S_L is still covered by the certificates of Z'.

The next lemma is fundamental for our inductive proof because it shows that each defining function of a bounding hyperplane of S_L must divide at least one of the functions used in any strict complete proof for L.

LEMMA 5.6. *Let Z be a strict complete proof for L with respect to Q with $S_L \neq \emptyset$. Let h be a bounding hyperplane of S_L with defining function l. Then there is a function g used in Z such that l divides g.*

Proof. Let $f = \prod_{g \in Z} g$. Then $f \not\equiv 0$. Assume that $f|_h \not\equiv 0$. Then there exists an $x \in h \cap \overline{S_L}$ with $f(x) \neq 0$ (by (F7) and (F4) and because h bounds S_L). But then there exists an $\varepsilon > 0$ such that all g in Z have a constant sign in $B_n(x, \varepsilon)$, which means that $B_n(x, \varepsilon) \subseteq S_L$ by (C1), a contradiction. Hence $f|_h \equiv 0$ and l divides f by (F6). But l is prime and hence divides one of the g in Z. ∎

COROLLARY 5.7. *Let Z be a strict complete proof for L with respect to Q with $S_L \neq \emptyset$. Let h be a bounding hyperplane of S_L with defining function l. Then there exists a strict complete proof Z' for L with respect to Q with $|Z'| \leqslant |Z|$ such that l divides some function used in Z' but l^2 does not divide any of the functions of Z'.*

Proof. First eliminate in Z all linear factors of multiplicity 2 or more, using Lemma 5.5; then apply Lemma 5.6. ∎

In this case we can prove that Reduction 5.3 works properly.

LEMMA 5.8. *Let Z be a strict complete proof for L with respect to Q with $S_L \neq 0$. Let h be a bounding hyperplane of S_L with defining function l. If l is unique in each certificate, where it appears as a linear factor, then Reduction 5.3, applied with hyperplane h, yields a strict complete proof Z' for L' with respect to Q'. Furthermore, $|Z'| \leqslant |Z| - 1$.*

Proof. $|Z'| \leqslant |Z| - 1$ follows directly from Lemma 5.4. It remains to show (C1) and (C2) for Z'. Let $Z = \{Z_1, ..., Z_p\}$ with $Z_i = (G_i, >)$ and $G_i = (g_{i1}, ..., g_{ik})$. By Lemma 5.4, we may assume that l divides g_{i1}; hence, $Z_i' = (G_{i,>}')$ with $G_i' = (g_{i2}|_h, ..., g_{ik}|_h)$ for all i. Furthermore, w.l.o.g. $l = l_1$, where $L = (l_1, ..., l_m)$, and hence, $L' = (l_2|_h, ..., l_m|_h)$:

(C1) Let $x \in S_{Z_i'}$ for an i. Then there exists an $\varepsilon > 0$ such that $h \cap B_n(x, \varepsilon) \subseteq S_{Z_i'} \subseteq \overline{S_{Z_i}}$ by Lemma 4.11. But then $l_i(x) \neq 0$ for $i \geqslant 2$ by Lemma 3.3(d) and, since $x \in \overline{S_L}$, even $l_i(x) > 0$. Hence $x \in S_{L'}$.

(C2) Let $x \in S_{L'} \subseteq \overline{S_L}$ with $Q'(x) \neq 0$. There exists a sequence $(x_s)_{s=1,2,...}$ with $x_s \in S_L$, $Q(x_s) \neq 0$, and $\lim_{s \to \infty} x_s = x$. For each x_s there is an index i_s such that $x_s \in S_{Z_{i_s}}$. Since we only have a finite number of certificates, one index must occur infinitely often in the sequence $(i_s)_{s=1,2,...}$. Let i be such an index.

So we have a subsequence $(y_s)_{s=1,2,...}$ of $(x_s)_{s=1,2,...}$ with $y_s \in S_{Z_i}$ and $\lim_{s \to \infty} y_s = x$. Hence, for all s, $g_{ij}(x_s) > 0$ for all j and therefore $g_{ij}(x) \geqslant 0$. Since $Q'(x) \neq 0$ we even have $g_{ij}(x) > 0$ for $j \geqslant 2$.

Assume $g_{i1}(x) > 0$. Then l does not divide any of the g_{ij} and hence, by Lemma 5.4, $S_{Z_i'} = \emptyset$, a contradiction. Therefore, $g_{i1}(x) = 0$ and l divides g_{i1} (otherwise, g_{i1} would be a factor of Q'; i.e., $Q'(x) = 0$, a contradiction). Therefore Z_i' exists and $x \in S_{Z_i'}$. ∎

Proof of Theorem 5.1. As mentioned before, we can assume that Z is a strict complete proof for $(L, >)$ and $S_{L,>} \neq \emptyset$ (Lemma 3.2). By Lemma 2.1(c) we know that there is a hyperplane h in L which bounds S_L and which contributes to a rank(L)-face in $\overline{S_L}$. Let l be the defining function of h. By Corollary 5.7 we can assume that l is a linear factor of some of the functions used in Z, but l^2 is not. We can even further assume that l is unique in each certificate of Z, where it appears as a linear factor (Lemma 4.8).

Now we can apply Reduction 5.3 to Z, L, and h and know by Lemma 5.8 that Z' is a strict complete proof for L' with respect to Q' with $|Z'| \leqslant |Z| - 1$. Furthermore, $\text{rank}(L') = \text{rank}(L)$. By induction hypothesis, $|Z'| \geqslant (n-1) - \text{rank}(L')$ and therefore $|Z| \geqslant 1 + |Z'| \geqslant n - \text{rank}(L)$. ∎

6. CONCLUSIONS

The proofs in this paper are mainly based on two techniques. One technique is to examine the number of free dimensions of the target set and the set of solutions for a certificate (Theorem 4.3). The other technique is not to stick to the given decision tree but to transform it into another decision tree with nicer properties and of at most the same depth (Ramanan proposed in [20], for example, to introduce artificial components, thus improving the classical lower bounds which are based on counting the number of connected components).

Yao's theorem cannot be generalized to, for example, quadratic polynomials, because two quadratic polynomials can have an arbitrarily small solution set which can be contained in any target set (see the example after Corollary 5.2). But other open problems from [28] are still waiting for an answer, for example, the question whether lower bound proofs for "simple" combinatorial problems (such as finding the k largest numbers) can always be carried out purely combinatorially, i.e., without the detour of geometric arguments.

At first glance it seems to be surprising that the methods used in the proof of Yao's theorem can also be used to prove Rabin's theorem. But a closer look at our proof of Rabin's theorem shows that we inductively prove the existence of a certificate with a set of solutions which is bordered by a rank(L)-face of Arr(H) and which uses the hyperplanes defining this rank(L)-face as linear factors (to be precise, we prove that there *could* be such a certificate). This is very similar to Yao's theorem.

In [19], Rabin gave as an example a problem, where the use of nonanalytic functions can beat his lower bound. A careful inspection of our proof (and Rabin's original proof) shows that the reason why the theorem fails in this case is the fact that the functions involved are not defined on the hyperplanes bounding the target set S_L. And in this case the inductive step which restricts everything to one of these bounding hyperplanes cannot work. This leads us to the following observation: We do not really require the functions used in a decision tree to satisfy the properties (F1)–(F6) everywhere in $\mathbb{R}^n$; it is sufficient if they are satisfied in a small environment around the rank(L)-face of S_L which is used in the inductive step. This is similar to the method of focusing on some convex set $C \subseteq \mathbb{R}^n$ in [19].

ACKNOWLEDGMENTS

We thank the unknown referees whose detailed comments helped us to improve the presentation of our results.

Received May 12, 1997; final manuscript received June 28, 1998

REFERENCES

1. Andradas, C., Bröcker, L., and Ruiz, J. M. (1988), Minimal generation of basic open semianalytic sets, *Invent. Math.* **92**, 409–430.
2. Ben-Or, M. (1983), Lower bounds for algebraic computation trees, *in* "Proceedings of the 15th ACM Symposium on the Theory of Computation (STOC '83)," pp. 80–86.

3. Björner, A., Lovász, L., and Yao, A. C. (1992), Linear decision trees: Volume estimates and topological bounds, *in* "Proceedings of the 24th ACM Symposium on the Theory of Computation (STOC '92)," pp. 170–177.
4. Bochnak, J., Coste, M., and Roy, M. F. (1984), Géométrie algébraique réelle, *in* "Ergebnisse der Mathematik und ihrer Grenzgebiete," Vol. 12, Folge 3, Springer-Verlag, Heidelberg.
5. Bröckner, L. (1984), Minimale Erzeugung von Positivbereichen, *Geom. Dedicata* **16**, 335–350.
6. Dobkin, D. P., and Lipton, R. J. (1979), On the complexity of computations under varying sets of primitives, *J. Comput. System Sci.* **18**, 86–91.
7. Edelsbrunner, H. (1987), Algorithms in combinatorial geometry, *in* "EATCS Monographs on Theoretical Computer Science," Vol. 10, Springer-Verlag, Heidelberg.
8. Fussenegger, F., and Gabow, H. N. (1979), A counting approach to lower bounds for selection problems, *J. Assoc. Comput. Mach.* **26**(2), 227–238.
9. Gasarch, W. I. (1991), On selecting the k largest with restricted quadratic queries, *Infortmation Processing Letters* **38**(4), 193–195.
10. Grigoriev, D., Karpinski, M., Meyer auf der Heide, F., and Smolensky, R. (1996), A lower bound for randomized algebraic decision trees, *in* "Proceedings of the 28th ACM Symposium on the Theory of Computation (STOC '96)," pp. 612–619.
11. Jaromczyk, J. W. (1981), An extension of Rabin's complete proof concept, *in* "Proceedings of the 10th International Symposium on the Mathematical Foundations of Computer Science (MFCS '81)," Springer Lecture Notes in Computer Science 118, pp. 321–326.
12. Manber, U., and Tompa, M. (1985), The complexity of problems on probabilistic, nondeterministic, and alternating decision trees, *Journal of the ACM* **32**(3), 720–732.
13. Mansour, Y., Schieber, B., and Tiwari, P. (1988), Lower bounds for integer greatest common divisor computations, *in* "Proceedings of the 29th Symposium on the Foundations of Computer Science (FOCS '88)," pp. 54–63.
14. Meyer auf der Heide, F. (1984), A polynomial linear search algorithm for the n-dimensional Knapsack problem, *Journal of the ACM* **31**(3), 668–667.
15. Meyer auf der Heide, F. (1985), Simulating probabilistic by deterministic algebraic computation trees, *Theoret. Comput. Sci.* **41**, 325–330.
16. Montaña, J. L., Pardo, L. M., and Recio, T. (1994), A note on Rabin's width of a complete proof, *Comput. Complexity* **4**, 12–36.
17. Moran, S., Snir, M., and Manber, U. (1985), Applications of Ramsey's theorem to decision tree complexity, *Journal of the ACM* **32**(4), 938–949.
18. Ó'Dúnlaing, C. (1988), A tight lower bound for the complexity of path-planning for a disc, *Information Processing Letters* **28**(4), 165–170.
19. Rabin, M. O. (1972), Proving simultaneous positivity of linear forms, *Journal of Computer and System Sciences* **6**, 639–650.
20. Ramanan, P. (1987), Obtaining lower bounds using artificial components, *Information Processing Letters* **24**(4), 243–246.
21. Recio, T., and Pardo, L. M. (1987), Rabin's width of a complete proof and the width of a semi-algebraic set, *in* "Proceedings of the European Conference on Computer Algebra," Leipzig, pp. 456–462.
22. Reingold, E. M. (1972), On the optimality of some set algorithms, *Journal of the ACM* **19**, 649–659.
23. Rivest, R., and Yao, A. C. (1980), On the polyhedral decision problem, *SIAM Journal on Computing* **9**, 343–347.
24. Snir, M. (1982), Comparisons between linear functions can help, *Theoretical Computer Science* **19**, 321–330.
25. Snir, M. (1985), Lower bounds on probabilistic linear decision trees, *Theoretical Computer Science* **38**, 69–82.

26. Steele, J. M., and Yao, A. C. (1982), Lower bounds for algebraic decision trees, *Journal of Algorithms* **3**, 1–8.

27. Strassen, V. (1983), The computational complexity of continued fractions, *SIAM Journal on Computing* **12**, 1–27.

28. Yao, A. C. (1989), On selecting the k largest with median tests, *Algorithmica* **4**(2), 293–300.

29. Yao, A. C. (1992), Algebraic decision trees and Euler characteristics, *in* "Proceedings of the 33rd Symposium on the Foundations of Computer Science (FOCS '92)," pp. 268–277.